1. Pätevätkö seuraavat kongruenssiyhtälöt ?

(a) $40 \equiv 13 \pmod 9$

(b) $211 \equiv 12 \pmod 2$

(c) $126 \equiv -46 \pmod 3$

(d) $29 \equiv -4 \pmod 7$

(e) $(10^{10} + 9) \equiv 49 \pmod{10}$

(f) $6^8 \equiv 2 \pmod 9$

Ratkaisu. (a) Kyllä, sillä $40 = 4 \cdot 9 + 4$ ja $13 = 9 + 4$.

(b) Ei, sillä 211 on pariton ja 12 parillinen.

(c) Ei, sillä 126 on jaollinen luvulla 3 mutta -46 ei ole.

(d) Ei, sillä $29 = 4 \cdot 7 + 1$ ja $-4 = -7 + 3$.

(e) Kyllä, sillä molempien lukujen viimeinen numero on 9.

(f) Ei, sillä 6^8 on jaollinen luvulla 9 ($6^8 = 2^8 \cdot 3^8 = 9 \cdot 2^8 \cdot 3^6$)

□

2. Muodosta renkaan $\mathbb{Z}_6$ yhteen-ja kertolaskutaulukot.

Ratkaisu. Yhteen-ja kerolasku taulukot ovat seuraavat:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

+	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

□

3. Määrää pienin positiivinen kokonaisluku m siten, että $m \equiv 7^{25} \pmod{11}$.

Ratkaisu. Ratkaisutapoja on monia, tässä yksi. Voidaan esittää luku 25 2-järjestelmässä lukuna $(11001)_2$, sillä $25 = 2^4 + 2^3 + 1 = 16 + 8 + 1$. Käydään läpi luvun 7 parillisia potensseja tarvittava määrä. Koska $7^2 = 49 \equiv 5 \pmod{11}$ niin tämän avulla $7^4 \equiv 5^2 \equiv 25 \equiv 3$, $7^8 \equiv 9$ ja $7^{16} \equiv 4$ Siispä

$$7^{25} \equiv 7^{16+8+1} \equiv 7^{16} \cdot 7^8 \cdot 7^1 \equiv 4 \cdot 9 \cdot 7 \equiv 3 \cdot 7 \equiv 10 \pmod{11}.$$

Tehtävässä kysytiin pienintä positiivista kokonaislukua jolla on sama jakojäännös, jaettaessa luvulla 11, kuin luvulla 7^{25}. Edellä lasketun nojalla pitää löytää pienin positiivinen kokonaisluku muotoa $11n + 10$, missä $n \in \mathbb{Z}$. Kysytty on luku 10. □

4. Määrää renkaan $\mathbb{Z}_{12}$ ne alkiot joilla on käänteisalkio, ja ilmoita kunkin käänteisalkio.

Ratkaisu. Luennolla esitellyn lauseen nojalla täsmälleen niillä alkiolla n on käänteisalkiot joille $\text{syt}(12, n) = 1$. Tässä niitä ovat $1, 5, 7, 11$. Alkion 1 käänteisalkio on aina luku itse. Lisäksi $5 \cdot 5 = 25 \equiv 1$, $7 \cdot 7 = 49 \equiv 1$ ja $11 \cdot 11 = 121 \equiv 1$ joten alkioiden 5, 7 ja 11 käänteisalkiot ovat luvut itse. □

5. Ratkaise yhtälö $13x \equiv 9$ renkaassa $\mathbb{Z}_{35}$.

Todistus. Huomataan ensimmäiseksi, että $\text{syt}(13, 35) = 1$ eli alkiolla 13 on käänteisalkio renkaassa $\mathbb{Z}_{35}$. Olkoon se b. Tällöin kongruenssien laskusääntöjen nojalla

$$x = b13x \equiv b9.$$

Etsitään b eukleideen algoritmilla:

$$\begin{aligned} 35 &= 2 \cdot 13 + 9 \\ 13 &= 9 + 4 \\ 9 &= 2 \cdot 4 + 1 \end{aligned}$$

Algoritmin peruuttaminen antaa

$$\begin{aligned} 1 &= 9 - 2 \cdot 4 \\ &= 9 - 2(13 - 9) \\ &= 3 \cdot 9 - 2 \cdot 13 \\ &= 3 \cdot (35 - 2 \cdot 13) - 2 \cdot 13 \\ &= 3 \cdot 35 - 8 \cdot 13. \end{aligned}$$

Erityisesti $-8 \cdot 13 \equiv 1$ eli $b \equiv -8 \equiv 27$. Nyt voimme ratkaista annetun yhtälön kuten alussa totesimme eli $x \equiv b9 \equiv 27 \cdot 9 \equiv 243 \equiv 33$. □

6. Onko luku $(((7^7)^7)^7)^7 + ((7^7)^7)^7$ jaollinen luvulla 10?

Ratkaisu. Huomataan, että $7^7 \equiv 823543 \equiv 3 \pmod{10}$ ja $(7^7)^7 \equiv 3^7 \equiv 2187 \equiv 7$ joten

$$(((7^7)^7)^7)^7 \equiv 7 \text{ ja } ((7^7)^7)^7 \equiv 3.$$

Summaamalla nämä yhteen näemme, että luku $(((7^7)^7)^7)^7 + ((7^7)^7)^7$ on jaollinen luvulla 10. □

7. Olet salakuunnellut Kallen ja Tiinan välistä viestittelyä ja pystynyt päättelemään heidän käyttävän RSA-salausmenetelmää julkisella avainparilla $N = 10001$ ja $e = 5$. Ratkaise näiden avulla purukuavain d, jolla pystyt lukemaan heidän koodaamat viestinsä.

Ratkaisu. RSA salauksessa käytetty luku N on kahden alkuluvun p ja q tulo. Tässä $N = 10001 = 73 \cdot 137$. Lisäksi salauksessa käytettiin apuna lukua

$$\psi = (73 - 1)(137 - 1) = 9792.$$

Jos heidän julkisen avaimen toinen pari (koodausavain) $e = 5$ niin tämä tarkoittaa sitä, että purukuavain on tämän käänteisalkio renkaassa $\mathbb{Z}_{9792}$. Ratkaistaan siis yhtälö

$$5x \equiv 1$$

kyseisessä renkaaassa. Tämä tapahtuu jälleen eukleideen algoritmilla:

$$9792 = 1958 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$

Peruutetaan algoritmi, jolloin

$$1 = 5 - 2 \cdot 2 = 5 - 2(9792 - 1958 \cdot 5) = 3917 \cdot 5 - 2 \cdot 9792.$$

Erityisesti

$$3917 \cdot 5 \equiv 1$$

ja siten ratkaisu $x \equiv 3917$. □

8. (Jatkoa..) Eräänä päivänä saat siepattua Tiinan lähettämän koodatun viestin

$$5003\ 6242\ 2088\ 6662\ 8831\ 8472.$$

Mitä viestissä sanotaan? (Käytä modululaskennassa apuna vaikka Wolfram Alpha tms. laskentaohjelmaa ja lopuksi muunna saadut numerot kirjaimiksi jotenkin..)

Ratkaisu. Edellisessä tehtävässä ratkaisimme purkuavaimen $d = 3917$. Tämän avulla voimme purkaa salauksen laskemalla viestissä esiintyville numerosarjoille (neljän numeron ketju) x

$$x^{3917} \pmod{10001}.$$

Tähän kannatta käyttää apuna esimerkiksi Wolfram Alpha sivustoa minne nämä voi suoraan tuossa muodossa ja se ymmärtää. Jos haluaa käyttää Pythonia apuna niin komento a % b laskee $a \pmod b$, tuo sama toimii myös Sagella (SageMath). Laskemalla nämä läpi kaikille viestissä esiintyville neljän numeron ryppäille saamme numerosarjat (samassa järjestyksessä)

$$191\ 201\ 131\ 111\ 215\ 16.$$

Yritetään kääntää tämä kirjaimiksi käyttäen hyväksi seuraavaa muuntotaulukkoa

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Q	R	S	T	U	V	W	X	Y	Z	Å	Ä	Ö			
17	18	19	20	21	22	23	24	25	26	27	28	29			

Tästä kun hetken miettii vaihtoehtoja niin huomaa, että jos viestissä lukee jotain selkokielistä niin täytyy numerosarjan jakaantua siten, että

$$19\ 1\ 20\ 1\ 13\ 1\ 11\ 12\ 15\ 16.$$

Tässä lukee siis, että "SATAMA KLO 16". □

9. Tarkastelemalla tilannetta sopivasti jäännöluokkien avulla näytä, että yhtälöllä $x^2 - 5y^2 = 2$ ei ole kokonaislukuratkaisuja.

Todistus. Tehdään antiteesi, että tällainen kokonaisluku löytyy. Olkoon se n. Tarkastellaan tilannetta jäännösluokassa $\mathbb{Z}_5$. Tällöin

$$2 \equiv n^2 - 5n^2 \equiv n^2.$$

Erityisesti on siis $n^2 \equiv 2$. (Eli kysymys palautuu siihen onko minkään luvun toisen potenssin jakojäännös, jaettaessa luvulla 5, luku 2.) Seuraava taulukko näyttää, että tämä ei ole mahdollista

n	n^2
0	0
1	1
2	4
3	4
4	1

joten saimme ristiriidan ja antiteesi on siis väärä.

□

10. ISSN on jatkuvasti ilmestyvän tekstijulkaisun kansainvälinen tunnus. Sen avulla tietty lehti, sarja tai muu jatkuva julkaisu voidaan yksiselitteisesti erottaa muista, jopa samannimisistä julkaisuista. ISSN koodit koostuvat kahdesta neljän numeron sarjasta $d_1d_2d_3d_4$-$d_5d_6d_7d_8$, missä viimeinen numero d_8 on niin sanottu tarkistusnumero. Tarkistusnumero toteuttaa kongruenssiyhtälön

$$d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}.$$

Jos $d_8 \equiv 10 \pmod{11}$ niin merkitään d_8 paikalle kirjain X.

(a) Onko koodi 1530-8669 validi ISSN koodi? Entä 1007-120X ? Ellei niin korjaa numero validiksi.

(b) Riittääkö tarkastusnumero paljastamaan kaikki mahdolliset virheet ISSN koodissa? (ts. määrääkö luku d_8 ISSN koodin yksikäsitteisesti?)

Ratkaisu. Koodille 1530-8669 saamme

$$3 + 20 + 15 + 0 + 56 + 48 + 54 = 196 \equiv 9 \pmod{11},$$

joten tarkastusnumero on oikein ja näin ollen koodi on validi. Koodille 1007-120X saamme

$$3 + 0 + 0 + 42 + 7 + 16 + 0 = 68 \equiv 2 \pmod{11},$$

joten tarkastusnumero ($X = 10$) ei ole oikein ja näin ollen koodi ei ole validi. Sen sijaan koodi 1007-1202 on validi. Kohtaa b) varten voi esimerkiksi huomata, että jos numeroihin d_3 ja d_4 lisää ykkösen niin summa $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7$ kasvaa yhdellätoista ja siten antaa saman tarkistusnumeron. Esimerkiksi koodit 1000-0011 ja 1011-0011 ovat validit ja niillä on sama tarkistusnumero. □